Pagers
Radios
Digital Cameras
Personal Digital Assistants such as Palm Pilots and Smart Phones
Portable storage devices such as USB thumb drives
Portable media devices such as iPods and MP3 players
Printers and copiers
Fax machines

Any component that is used to build or support the Kern Community College District network including, but not limited to:

Routers
Switches
Servers
Enterprise Storage Systems
Microwave Components
Firewalls
Cabling Infrastructure
Wireless Access Points and Controllers
Telephone Switches
Voicemail Systems
Network Management and Monitoring Systems

**3E2** Attaching Outside Agencies to the District Wide Area Network (WAN)

3E2A The Kern Community College District (KCCD) may attach outside agencies to the District Wide Area Network (WAN) when such attachments are mutually beneficial, and consistent with the purposes of the District and its Colleges. These agencies may include, but are not limited to, school districts, hospitals, and police and fire departments.

3E2B The proposal to attach to the District WAN shall be put in the form of a written agreement or contract, and approved by the Board of Trustees or its designee.

3E2C Written proposals will follow the Procedures for implementing these Policies. [See Procedure 3E2E of this Manual for Attaching Outside Agencies to the District-wide Area Network (WAN).]

**3E3** Electronic Mail Policy

See Procedure 3E3 of this Manual for the Electronic Mail Procedure and Appendix 3E3 for References and Definitions Pertaining to Mail. (Added August 3, 2000)

3E3A The Kern Community College District (KCCD) recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. There is, however, no absolute right to such privacy provided by law;

information retained on, or transmitted via, an employer's computer systems is considered the property of the employer.

3E3B KCCD encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder's consent. Subject to the requirements for authorization, notification, and other conditions specified in the accompanying Procedure, KCCD may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail (a) when required by and consistent with law; (b) when there is substantiated reason to believe that violations of law or of KCCD policies have taken place; (c) when there are compelling circumstances; or (d) under time-dependent, critical operational circumstances.

## 3E4 Security Policy *(Added July 9, 2009)*

### 3E4A Introduction

Kern Community College District has an obligation to ensure that all Information Technology data, equipment, and processes in its domain of ownership and control are properly secured. This obligation is shared, to varying degrees, by the Colleges and their Centers and every employee of the Kern Community College District. Meeting this obligation is critical to achieving Kern Community College District's mission of providing outstanding educational programs and services that are responsive to our diverse students and communities.

In order to carry out its mission, Kern Community College District shall provide secure yet open and accessible Information Technology resources to all employees and students. Toward this end, Kern Community College District will strive to balance its Information Technology Security Program efforts with identified risks that threaten the availability and performance of mission critical computing and network resources.

Kern Community College District shall ensure that the use of Information Technology resources complies with the appropriate Kern Community College District policies and procedures and applicable Federal and State regulations.

#### 3E4A1 Definitions

a. Information Technology Resources: people, processes, and technology needed to deliver Information Technology services (Banner, e-mail, online classes, etc.) to Kern Community College District employees and students.

b. Computing and Network Resources: any and all technology (servers, personal computers, applications, laptops, routers, etc.) that make up Kern Community College District's vast Information Technology operation.

## 3E4B Scope of Information Technology Security

### 3E4B1 Information Technology Security Defined

Information Technology Security is defined as the state of being relatively free of risk. This risk concerns the following categories of losses:

a. Confidentiality of Information Technology data or privacy of personal data and college data

b. Integrity or accuracy of personal data and college data stored in Information Technology systems

c. Information Technology assets which include Information Technology systems, networks, facilities, programs, documentation, and data

d. Personal and college data stored in Information Technology systems

Information Technology Security is also viewed as balancing the implementation of security measures against the risks that have been identified and weighted against the effective operation of the Kern Community College District.

### 3E4B2 Domains of Information Technology Security

Kern Community College District's Information Technology Security shall deal with the following domains of security:

a. Computer Systems' Security: servers, workstations, applications, laptops, mobile devices, operating systems, and related peripherals used by Kern Community College District employees and students

b. Network and Communications Security: all equipment, people, and processes in place to operate Kern Community College District's network and communications infrastructure

c. Physical Security: premises occupied by Information Technology personnel and core (not end-user) Information Technology equipment such as servers, routers, and switches

d. Operational Security: environmental systems such as HVAC, power, and other related operational systems

### 3E4B3 Information Technology Security Program

Kern Community College District shall have an Information Technology Security Program comprised of the following components:

a. A framework for classifying, reviewing, and updating Kern Community College District's Security risk posture (Risk Assessment)

A framework for identifying location, type, sensitivity, and access requirements for all data residing anywhere within the Kern Community College District

Documentation of Information Technology Security Program roles, responsibilities, processes, and architecture

A plan for identifying, prioritizing, and addressing applicable Federal, State, and other legal compliance requirements

Appropriate Information Technology Security policies, procedures, and guidelines

An Information Technology Security Awareness and Information Dissemination plan

A plan for identifying, validating, prioritizing, implementing, and auditing Information Technology security technology initiatives needed to effectively secure Kern Community College District's Information Technology operations

3E4C Roles and Responsibilities

3E4C1 Within the context of Information Technology Security, all Kern Community College District employees and students are responsible to some degree for safeguarding the Information Technology resources they use. Equally, all Kern Community College District employees and students are expected to comply with all Kern Community College District Information Technology Security policies and related procedures.

3E4C2 The Information Technology Managers from the three Colleges and the District Office are responsible for Information Technology Security throughout Kern Community College District.

3E4C3 Kern Community College District's Director, Information Technology is responsible for carrying out Kern Community College District's Information Technology Security Program as outlined in Policy 3E4B3 .

3E4C4 Appropriate College and District-wide committees shall have the opportunity to provide input on the development of Information Technology Security policies and procedures.

3E4D Sanctions

3E4D1 Violations of this policy are subject to the established Kern Community College District disciplinary processes as outlined in Kern Community College District Board Policy and Kern Community College District employee contracts.

Acknowledgements: Kern Community College District acknowledges Murdoch University of Perth, Western Australia (www.murdoch.edu.au), and the University of Minnesota (www.umn.edu) for allowing Kern Community College District to use their Information Technology Security policy material.

## 3E5 Wireless Communication Devices *(Added December 17, 2009)*

### 3E5A Introduction

3E5A1 The Kern Community College District recognizes that certain specific job functions require the use of wireless communication devices to conduct official business. When the job duties of an employee require the use of a wireless communication device to conduct District business, the Chancellor or President may provide the employee with a wireless communication device or allowance. (See Procedure 3E5)

### 3E5B Use

3E5B1 No personal calls may be initiated or received on District issued devices. Personal use may result in disciplinary action.

3E5B2 Use of wireless communication devices is prohibited while driving District vehicles and while driving any vehicle during the course or scope of employment. There are no exceptions, including hands-free devices.

3E5B3 Any personal use of wireless communication devices, including text messaging, during scheduled work hours shall be kept to a minimum or made on the employee's own time.

### 3E5C Issuance

3E5C1 If an employee receives a District allowance, the allowance will be taxable income to the employee.

3E5C2 If the District-issued wireless communication device is lost, damaged, or stolen, the employee is responsible for notifying the Help Desk immediately to prevent unauthorized use of the wireless communication device.

3E5C3 The District or College-issued wireless communication devices will be returned if the employee discontinues employment with the District or College.

3E5D Definition

3E5D1 Wireless communication devices include:

Pager
Push-to-Talk
Cell Phone
Push-to-Talk with Cell Service
SmartPhone

**Procedure 3E2E**

# Attaching Outside Agencies to the District Wide Area Network (WAN)

1. A written proposal to attach outside agencies to the District WAN is required, and must meet the following stipulations:

a) Cite and explain the mutual benefit to the District and the outside agency of the proposed attachment.

b) Identify the costs required to establish and maintain the proposed attachment with the assistance of the District Information Technology staff. Cost considerations should include, but not be limited to, the following:

- Hardware costs
- Support costs
- Bandwidth costs
- Personnel costs
- Other costs

c) Propose the method for either recovering the related costs, and/or demonstrating the quantifiable off-setting financial benefits to the KCCD.

d) Specify the proposed terms and conditions, which include the following:

- Duration of the agreement and means for evaluating whether it should be extended, renewed, or terminated
- Services to be provided
- Costs to the District and method of cost recovery and/or reimbursement
- Disclaimers related to the interruptions outside the control of KCCD
- Mutually agreed upon security provisions
- Method of distribution of resources and obligations upon dissolution of agreement

2) A proposal following the stipulations set forth in the Procedures noted in #1, above, will be presented to the District-wide Information Technology Committee (DWITC) for consideration, with action following at a subsequent meeting.

3) The DWITC recommendation will be taken to the Chancellor's Cabinet for consideration.

4) The agreement or contract for attaching the outside agency to the District WAN will be taken to the Board of Trustees for action upon the recommendation of the Chancellor's Cabinet.

5) Once the proposal to attach an outside agency to the District WAN is approved, the Assistant Chancellor, Information Technology will implement the agreement and proceed with the project.

Approved by the Chancellor's Cabinet
February 8, 2000

**Procedure 3E3**

# Electronic Mail Procedure

## PART ONE--INTRODUCTION

The purpose of this Procedure is to assure that:

1. The Kern Community College District (KCCD) community is informed about the applicability of policies and laws to electronic mail;

2. Electronic mail services are used in compliance with those policies and laws;

3. E-mail users are informed about how concepts of privacy and security apply to electronic mail; and

4. Disruptions to KCCD electronic mail and other services and activities are minimized.

## PART TWO--DEFINITIONS

***Any readers unfamiliar with the terminology used in this Procedure can refer to a set of definitions in*** *Appendix 3E3****, Part C.***

## PART THREE--GENERAL INFORMATION

General information regarding electronic mail has been included **in** **Appendix 3E3**, Part D.

## PART FOUR--SCOPE

This Procedure applies to:

1. All electronic mail systems and services provided or owned by the KCCD.

2. All users, holders, and uses of KCCD E-mail services.

3. All KCCD E-mail records in the possession of KCCD employees or other E-mail users of electronic mail services provided by the KCCD.

This Procedure applies only to electronic mail in its electronic form. The Procedure does not apply to printed copies of electronic mail.

## PART FIVE--GENERAL PROVISIONS

1. **Purpose**--In support of its mission of instruction and public service, the KCCD encourages the use of KCCD electronic mail services to share information, to improve communication, and to exchange ideas.

2. **KCCD Property**--KCCD electronic mail systems and services are KCCD facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with KCCD, or any sub-unit of the KCCD, assigned by the KCCD to individuals, sub-units, or functions of the KCCD, is the property of the KCCD.

3. **Service Restrictions**--Those who use KCCD electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of KCCD, and with normal standards of professional and personal courtesy and conduct. Access to KCCD electronic mail services is a privilege that may be wholly or partially restricted by KCCD without prior notice and without the consent of the E-mail user when required by and consistent with law, when there is substantiated reason (as defined in **Appendix 3E3**, Part C, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs.

4. **Consent and Compliance**--An E-mail holder's consent shall be sought by KCCD prior to any inspection, monitoring, or disclosure of KCCD E-mail records in the holder's possession, except as provided for in Part Five, Number 5. KCCD employees are, however, expected to comply with KCCD requests for copies of E-mail records in their possession that pertain to the administrative business of KCCD, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by KCCD. Failure to comply with such requests can lead to the conditions of Part Five, Number 5.

5. **Restrictions on Access Without Consent**--KCCD shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such E-mail (a) when required by and consistent with law; (b) when there is substantiated reason (as defined in **Appendix 3E3**, Part C, Definitions) to believe that violations of law or KCCD policies listed in **Appendix 3E3**, Part B have taken place; (c) when there are compelling circumstances as defined in Part Three; or (d) under time-dependent, critical operational circumstances as defined in Appendix 3E3, Part C, Definitions.

   When the contents of E-mail must be inspected, monitored, or disclosed without the holder's consent, the following shall apply:

   (A) Authorization--Except in emergency circumstances as defined in **Appendix 3E3**, Part C, Definitions, and pursuant to Part Five, Number 5b, such actions must be authorized in advance and in writing by KCCD Assistant Chancellor for Information Technology Services (IT). Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

   (B) Emergency Circumstances--In emergency circumstances as defined in **Appendix 3E3**, Part C, Definitions, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Part Five, Number 5A, above.

Part Five, Number 5 (continued)

(C) Notification--In either case, the responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with other KCCD policies and procedures, notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

(D) **Compliance with Law**--Actions taken under Part Five, Numbers 1 and 2 shall be in full compliance with the law and other applicable KCCD policy and procedure, including laws and policies listed in **Appendix 3E3**, Part A.

6. **Recourse**--Individuals who believe that actions taken by employees or agents of KCCD were in violation of this Procedure should file a complaint with the Assistant Chancellor for IT.

7. **Misuse**--In general, both law and KCCD policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to electronic mail services and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies (see **Appendix 3E3**, Part A, References).

## PART SIX--SPECIFIC PROVISIONS

1. **Allowable Use**--In general, use of KCCD electronic mail services is governed by policies that apply to the use of all KCCD facilities. In particular, use of KCCD electronic mail services is encouraged and is allowable subject to the following conditions:

(A) Purpose--Electronic mail services are to be provided by KCCD organizational units in support of the teaching, research, and public service mission of KCCD, and the administrative functions that support this mission.

(B) Users--Users of KCCD electronic mail services are to be limited primarily to KCCD students, faculty, staff, and community users for purposes that conform to the requirements of this Section.

(C) Non-Competition--KCCD electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the KCCD.

(D) Restrictions--KCCD electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of KCCD; personal financial gain (see applicable academic personnel policies); personal use inconsistent with Part Six, Number 1H; or uses that violate other KCCD policies or guidelines. The latter include, but are not limited to, policies and guidelines (see **Appendix 3E3**, Part A, References) regarding intellectual property, or regarding sexual or other forms of harassment.

(E) Representation--Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of KCCD or any unit of KCCD unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing KCCD. (e.g., "These opinions are my own, not those of KCCD.")

(F) False Identity--KCCD E-mail users shall not employ a false identity. E-mail may, however, be sent anonymously, provided this does not violate any law or any KCCD policy, and does not unreasonably interfere with the administrative business of KCCD.

(G) Interference--KCCD E-mail services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of E-mail or E-mail systems. Such uses include, but are not limited to, the use of E-mail services to: (a) send or forward E-mail chain letters; (b) "spam," that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited E-mail; and (c) "letter-bomb," that is, to resend the same E-mail repeatedly to one or more recipients to interfere with the recipient's use of E-mail.

(H) Personal Use--KCCD electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (i) directly or indirectly interfere with the KCCD operation of computing facilities or electronic mail services; (ii) burden the KCCD with noticeable incremental cost; or (iii) interfere with the E-mail user's employment or other obligations to the KCCD.

## 2. Security and Confidentiality

(A) The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Procedure, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using E-mail to communicate confidential or sensitive matters.

(B) Users should be aware that, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of KCCD E-mail services, and on these and other occasions may inadvertently see the contents of E-mail messages. Except as provided elsewhere in this Procedure, they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise

Part Six, Number 2B (continued)

use what they have seen. One exception, however, is that of systems personnel (such as "postmasters") who may need to inspect E-mail when re-routing or disposing of otherwise undeliverable E-mail. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable E-mail to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the E-mail has been inspected for such purposes.

(C) The KCCD attempts to provide secure and reliable E-mail services. Operators of KCCD electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of E-mail services have no control over the security of E-mail that has been downloaded to a user's computer. As a deterrent to potential intruders and to misuse of E-mail, E-mail users should employ whatever protections (such as passwords) are available to them.

(D) Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies that can be retrieved. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process copies data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail.

## 3. Archiving and Retention

(A) KCCD does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up only to assure system integrity and reliability, not to provide for future retrieval. Operators of KCCD electronic mail services are not required by this Procedure to retrieve E-mail from such back-up facilities upon the holder's request, although on occasion they may do so as a courtesy.

(B) E-mail users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms, such as compound documents composed of digital voice, music, image, and video in addition to text. Furthermore, in the absence of the use of authentication systems (see Part One, Number 4), it is difficult to guarantee that E-mail documents have not been altered, intentionally or inadvertently.

Part Six, (continued)

(C) E-mail users and those in possession of KCCD records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid-free paper or microfilm, where long-term accessibility is an issue.

## PART SEVEN--PROCEDURE VIOLATIONS

Violations of KCCD procedures governing the use of KCCD electronic mail services may result in restriction of access to KCCD information technology resources. In addition, disciplinary action, up to and including dismissal, may be applicable under other KCCD policies, guidelines, implementing procedures, or collective bargaining agreements.

## PART EIGHT--RESPONSIBILITY FOR PROCEDURE

The Assistant Chancellor for IT is responsible for development and maintenance of this Procedure, with the concurrence of the District-Wide IT Committee (DWITC).

Approved by Chancellor's Cabinet
March 28, 2000

**Procedure 3E5**

# Wireless Communication Devices

1. All employees who require the use of a wireless communication device to conduct District business must complete and submit the Kern Community College District Wireless Communication Device Authorization Request form. (See **Appendix 3E5**)

Reviewed and Recommended by
Chancellor's Cabinet
November 18, 2008

Reviewed and Recommended by
District Consultation Council
October 27, 2009